UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/671,388	09/27/2000	Michael Ginsberg	MS150832.2	6789

27195 7590 11/25/2003

AMIN & TUROCY, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
OSMAN, AHMED A	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 11/25/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/671,388	GINSBERG, MICHAEL	
	Examiner	Art Unit	
	Ahmed A Osman	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED OFFICE ACTION

1. Claims 1-20 are presented for examinations.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "40" and "48" have both been used to designate Files Section. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

3. Claim 17 recites the limitation "the program" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section

351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-5, 7-8, 10, 12-14, and 17-19 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by U.S. Patent No. 6,289,462 to McNabb.

As per claim 1:

"A system for regulating access to a platform"

McNabb teaches a method for assigning control and access attributes to data objects for a commercial software product executing on a trusted server (Claim 1 preamble).

"A component for analyzing a first module and an application environment associated with the first module"

McNabb teaches a component of the present invention whose function is to examine each incoming request and decide which application should handle it (Column 8 Line 51).

"Determining the level of access to the platform"

McNabb teaches a method where a trusted server determines extended attributes to be applied to the processes and the data files of the commercial software product (Column 23 Line 49).

"Applying a trust level to the first module corresponding to the determined level of access"

McNabb teaches a method where a trusted server applies the determined extended attributes for the received administrator sensitivity level to the processes and data components of the commercial software products (Column 23 Line 53).

As per claim 2:

"The system of claim 1, the component for analyzing the first module providing for inheritance of the trust level"

McNabb teaches a trusted server system, which includes a link to retrieve previously, stored attribute label information related to the file (Column 10 Line 63).

As per claim 3:

"The system of claim 1, the component for analyzing the first module providing for marking the first module with at least one of states: (1) fully trusted, (2) run restricted, and (3) fail to load"

Figure 10 of McNabb shows the different Sensitivity Labels to be applied. Figure 11 of McNabb illustrates the process in which permission is granted according to the label given from Figure 10. In Figure 11, it is clear that according to the label applied, the 3 permission levels, are to deny permission, run with only innate privileges, and run with authorized privileges and innate privileges. Those 3 states correspond to the 3 proposed labels claimed here, which are fully trusted, run restricted, and fail to load. Examiner concludes that the 3 labels serve the same purpose and the difference in terminology is just the inventors' choice of words.

As per claim 4:

"The system of claim1, wherein the component is stored in a Read Only Memory (ROM) in the platform"

McNabb teaches that the processes or components of the present disclosed system may be implemented using software components, or may alternatively utilize microprocessors having embedded Processes. McNabb further teaches a process table, which is part of the disclosed invention, is an encrypted file stored on the trusted server that is a read only data structure (Column 18 Line 20). The examiner concludes that a component of the disclosed invention may be stored in a read only memory in the platform.

As per claim 5:

"The system of claim 1, wherein the component is part of an operating system"

McNabb teaches the present invention shown in Figure 1 requires that modifications to the operating system are incorporated such that the operation of key components are affected (Column 8 Line 54).

As per claim 7:

"The system of claim 1, wherein the functionality of one or more Application Programming Interface (API) calls, when called by the first module, are selectively restricted"

McNabb teaches a trusted server that will direct an anonymous user to a partition where the user request is assigned a low level sensitivity label. The separate partition exclusively restricts the available processes and files that may be executed or viewed (Column 18 Line 7). McNabb adds an example of the disclosed invention where the process stages may be established to selectively lock or freeze access to certain process execution steps or data access abilities, where users may have total privileges at one point in the process and later have none or read only ability on the data or execution of processes (Column 20 Line 33).

As per claim 8:

"The system of claim 7, wherein selectively restricting the functionality of the one or more API calls includes restricting the functionality to read functions."

McNabb teaches other restrictions implemented to secure the operating system of the disclosed invention require the segmentation of the superuser privilege (Column 12 Line 50). McNabb further states that the backup program may be able to read any file, but it cannot be exploited to shut down the system, modify files, or send random network packets (Column 12 Line 53). Moreover, McNabb adds an example of the disclosed invention where the process stages may be established to selectively lock or

freeze access to certain process execution steps or data access abilities, where users may have total privileges at one point in the process and later have none or read only ability on the data or execution of processes (Column 20 Line 33). Therefore restricting the functionality to read functions.

As per claim 10:

"Means for determining a trust level for a first module"

McNabb teaches a method where a trusted server determines extended attributes to be applied to the processes and the data files of the commercial software product (Column 23 Line 49).

"Means for applying the trust level to the first module to regulate access to the platform"

McNabb teaches a method where a trusted server applies the determined extended attributes for the received administrator sensitivity level to the processes and data components of the commercial software products (Column 23 Line 53).

As per claim 12:

"Determining a trust level for a first module"

McNabb teaches a method where a trusted server determines extended attributes to be applied to the processes and the data files of the commercial software product (Column 23 Line 49).

"Applying the trust level to the first module to regulate access to the platform"

McNabb teaches a method where a trusted server applies the determined extended attributes for the received administrator sensitivity level to the processes and data components of the commercial software products (Column 23 Line 53).

As per claim 13:

"The method of claim 12 wherein determining the trust level for the first module further comprises the step of marking the first module with at least one of states: (1) fully trusted, (2) run restricted, (3) fail to load"

Figure 10 of McNabb shows the different Sensitivity Label to be applied. Figure 11 of McNabb illustrates the process in which permission is granted according to the label given from Figure 10. In Figure 11, it is clear that according to the label applied, the 3 permission levels, are to deny permission, run with only innate privileges, and run with authorized privileges and innate privileges. Those 3 states correspond to the 3 proposed labels claimed here, which are fully trusted, run restricted, and fail to load. Examiner concludes that the 3 labels serve the same purpose and the difference in terminology is just the inventors' choice of words.

As per claim 14:

"The method of claim 12 wherein determining the trust level for the first module further comprises transmitting the first module to a verification program"

McNabb teaches that the functionality afforded by the disclosed invention is therefore to extend the verification of process-to-process communications where each process is compared to the role of the user, and the privileges permitted for the processes (Column 14 Line 44). McNabb further states that the permission bits are checked at step 600, then at step 604 Sensitivity Level (SL) labels are verified to establish that the process SL (272) is equal to or greater than the file SL (292) (Column 14 Line 62).

As per claim 17:

"The method of claim 12 wherein the program for determining the trust level for the first module is stored in a ROM in the platform"

McNabb teaches that the processes or components of the present disclosed system may be implemented using software components, or may alternatively utilize microprocessors having embedded Processes. McNabb further teaches a process table, which is part of the disclosed invention, is an encrypted file stored on the trusted server that is a read only data structure (Column 18 Line 20). The examiner concludes that a component of the disclosed invention may be stored in a read only memory in the platform.

As per claim 18:

"The method of claim 12 wherein the logic for applying the trust level to regulate access to the platform is stored in a ROM in the platform"

McNabb teaches that the processes or components of the present disclosed system may be implemented using software components, or may alternatively utilize microprocessors having embedded Processes. McNabb further teaches a process table, which is part of the disclosed invention, is an encrypted file stored on the trusted server that is a read only data structure (Column 18 Line 20). The examiner concludes that a component of the disclosed invention may be stored in a read only memory in the platform.

As per claim 19:

"The method of claim 12 wherein the trust level may be inherited"

McNabb teaches a trusted server system, which includes a link to retrieve previously, stored attribute label information related to the file (Column 10 Line 63)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 6, 9, 11, 15-16, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,289,462 to McNabb in view of U.S. Patent No. 6,546,487 to McManis.

As per claim 6:

"The system of claim 1, wherein the trust level is utilized to regulate access to the platform of one or more second modules called by the first module."

McNabb fails to mention any access regulation regarding one or more second modules called by the first module. McManis teaches a computer system where a second program module includes an executable procedure to be performed in response to the procedure call by the first program module to the second module. A procedure call to the program module verifier that is logically positioned in the second program module so as to be executed prior to completion of execution of the second program module's executable procedure, and instructions preventing completion of execution of that executable procedure when the program module verifier returns a verification denial with respect to the first program module (Column 2 Line 18). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of McNabb to regulate access to one or more second modules called by the first module. One would have been motivated to make such a modification in view of the suggestion by McNabb that it is desirable that the request by a user may only initiate predefined processes where the authorization to perform a process is

verified at each process step, and where the process does not inherit rights or pass rights to other subsequent processes (Column 4 Line 46).

As per claim 9:

"The system of claim 8, wherein selectively restricting the functionality of the one or more API calls includes terminating the first module."

McNabb fails to mention any restrictions on the functionality of the API calls. McManis teaches a method or procedure 128 which includes at least one verifier procedure call instruction 130 and instructions 132 for responding to a verification denial message received in response to the verifier procedure call, such as instructions for aborting execution of the procedure (Column 3 Line 14). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of McNabb to selectively restrict the functionality of API calls to abort the execution. One would have been motivated to make such a modification to maintain a secure operating system where access is strictly controlled and where the processing is restricted to permit only those actions required to respond to the request, according to McNabb (Column 4 Line 34).

As per claim 11:

"The system of claim 10 further comprising means for applying the trust level to one or more second modules called by the first module"

McNabb fails to mention any access regulation regarding one or more second modules called by the first module. McManis teaches a computer system where a second program module includes an executable procedure to be performed in response to the procedure call by the first program module to the second module. A procedure call to the program module verifier that is logically positioned in the second program module so as to be executed prior to completion of execution of the second program module's executable procedure, and instructions preventing completion of execution of that executable procedure when the program module verifier returns a verification denial with respect to the first program module (Column 2 Line 18). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of McNabb to regulate access to one or more second modules called by the first module. One would have been motivated to make such a modification in view of the suggestion by McNabb that it is desirable that the request by a user may only initiate predefined processes where the authorization to perform a process is verified at each process step, and where the process does not inherit rights or pass rights to other subsequent processes (Column 4 Line 46).

As per claim 15:

"The method of claim 12 wherein regulating access to the platform further comprises selectively aborting calls made to one or more APIs."

McNabb fails to mention any restrictions on the functionality of the API calls. McManis teaches a method or procedure 128 which includes at least one verifier

procedure call instruction 130 and instructions 132 for responding to a verification denial message received in response to the verifier procedure call, such as instructions for aborting execution of the procedure (Column 3 Line 14). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of McNabb to selectively restrict the functionality of API calls to abort the execution. One would have been motivated to make such a modification to maintain a secure operating system where access is strictly controlled and where the processing is restricted to permit only those actions required to respond to the request, according to McNabb (Column 4 Line 34).

As per claim 16:

"The method of claim 12 wherein regulating access to the platform further comprises selectively terminating the first module"

McNabb fails to mention any restrictions on the functionality of the API calls. McManis teaches a method or procedure 128 which includes at least one verifier procedure call instruction 130 and instructions 132 for responding to a verification denial message received in response to the verifier procedure call, such as instructions for aborting execution of the procedure (Column 3 Line 14). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of McNabb to selectively restrict the functionality of API calls to abort the execution. One would have been motivated to make such a modification to maintain a secure operating system where access is strictly controlled and where the processing

is restricted to permit only those actions required to respond to the request, according to McNabb (Column 4 Line 34).

As per claim 20:

"The method of claim 12 wherein the trust level may be applied to one or more second modules called by the first module."

McNabb fails to mention any access regulation regarding one or more second modules called by the first module. McManis teaches a computer system where a second program module includes an executable procedure to be performed in response to the procedure call by the first program module to the second module. A procedure call to the program module verifier that is logically positioned in the second program module so as to be executed prior to completion of execution of the second program module's executable procedure, and instructions preventing completion of execution of that executable procedure when the program module verifier returns a verification denial with respect to the first program module (Column 2 Line 18). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of McNabb to regulate access to one or more second modules called by the first module. One would have been motivated to make such a modification in view of the suggestion by McNabb that it is desirable that the request by a user may only initiate predefined processes where the authorization to perform a process is verified at each process step, and where the process does not inherit rights or pass rights to other subsequent processes (Column 4 Line 46).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following patents are cited to further show the state of the art with respect to trust level analysis in general:

U.S. Patent No. 5,675,782 to Montague et al.

U.S. Patent No. 5,933,498 to Schneck et al.

U.S. Patent No. 5,958,050 to Griffin et al.

U.S. Patent No. 6,505,300 to Chan et al.

U.S. Patent No. 6,523,120 to Strasnick

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ahmed A Osman whose telephone number is 703-305-8910. The examiner can normally be reached on Monday-Friday from 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 703-305-9595. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

***

EMMANUEL L. MOISE
PRIMARY EXAMINER
AU 2133

Ahmed Osman

United States Patent & Trademark Office

Patent Examiner – AU 2133

November 14, 2003